WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Term	Documents
(5 AND 7).USPT.	8
(L7 AND L5).USPT.	8

Database: US Patents Full-Text Database; US Pre-Grant Publication Full-Text Database; JPO Abstracts Database; EPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search: L8

Refine Search | Recall Text | Clear

Search History

DATE: Thursday, June 12, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L8	L7 and L5	8	L8
L7	L1 and (resource$ with (access$ adj2 control$))	355	L7
L6	L1 and (resource$ and (access$ adj2 control$))	2963	L6
L5	L1 and (resource$ adj3 provider$)	97	L5
L4	L2 and L3	0	L4
L3	L1 and (resource$ and (access$ adj2 control$)).ab.	66	L3
L2	L1 and (resource$ adj3 provider$).ab.	15	L2
L1	(709/$ OR 707/$ OR 705/$).CCLS.	31831	L1

END OF SEARCH HISTORY

L8: Entry 1 of 8 File: USPT Nov 12, 2002

DOCUMENT-IDENTIFIER: US 6480861 B1
TITLE: Distributed adaptive computing

Brief Summary Text (13):
Pursuant to one common prior art approach, the management of access to system resources in a distributed environment may be conducted by ascertaining the rights and privileges of a service requestor at the time that a service request is received. If a requestor's privileges are sufficient to allow execution of the request for service provision, the request proceeds. Requestors with insufficient privileges are not granted access to a service. Using this approach, access to a system resource is binary: based upon the identity of the service provider, the request is either granted or not granted. Access privileges to system resources are typically defined and assigned by an administrator. The administrator grants these privileges to requesting entities in an effort to anticipate access requirements in advance of actual service requests. While this method of access control is well-suited to the provision of system security, it is deficient when applied to resource allocation. The assignment of privileges to regulate access to resources is essentially an effort to early-bind the set of resources to a service requestor. Such an assignment shares the same set of design deficits as the early binding technique described above.

Brief Summary Text (15):
Other prior art approaches have dealt with selecting appropriate physical locations for applications on a network so as to enhance system performance. The physical location of an application on a network directly impacts the response time of that application. Services installed on under-utilized resources execute faster than identical services installed on busy resources. The topological proximity of a service to its potential requestors and the proximity of system resources necessary for the delivery of that service directly affect the response time of that service. Ideally, the decision of where an instance of a service ought to be installed takes into account the location of the community of service requestors, available bandwidth, the proximity of data and third party services, and the load on the server where the services run. At present, this decision is typically made by system administrators and is adjusted as new applications, resources and demands are made of the system. Unfortunately, as in the case of resource allocation, decisions pertaining to resource location are also labor-intensive and subject to similar constraints. However, the locations of system resources, service providers, and service points are not readily changeable so as to provide for optimization under a variety of conditions. This is compounded by the difficulty associated with gathering statistics and measures to determine if the location of a service is inefficient and if so, where to relocate the service in order to maximize efficiency.

Current US Original Classification (1):
707/103Y

Current US Cross Reference Classification (1):
705/400

Current US Cross Reference Classification (2):
705/80

Current US Cross Reference Classification (3):
707/10

Current US Cross Reference Classification (4):
709/202

US006480861B1

(12) **United States Patent**
Kanevsky et al.

(10) **Patent No.: US 6,480,861 B1**
(45) **Date of Patent: Nov. 12, 2002**

(54) **DISTRIBUTED ADAPTIVE COMPUTING**

(75) Inventors: **Paul Kanevsky**, Lawrenceville; **Anthony C. Pizi**, Cranbury; **Thomas Tsao**, Princeton Junction; **Daniel Tyler**, Lambertville, all of NJ (US)

(73) Assignee: **Merrill Lynch, Co., Inc**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/258,711**

(22) Filed: **Feb. 26, 1999**

(51) **Int. Cl.**[7] **G06F 17/30**

(52) **U.S. Cl.** **707/103**; 707/10; 705/80; 705/400; 709/202

(58) **Field of Search** 707/10, 104, 103; 705/70, 79, 80, 10, 34, 35, 400; 709/229, 203, 217, 202

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,940,815 A	*	8/1999	Maeda et al.	706/12
6,049,819 A	*	4/2000	Buckle et al.	709/202
6,078,906 A	*	6/2000	Huberman	705/37
6,084,874 A	*	7/2000	Nyguyen et al.	370/352
6,115,712 A	*	9/2000	Isam et al.	707/10
6,167,449 A	*	12/2000	Arnold et al.	709/227
6,178,406 B1	*	1/2001	Cheetham et al.	705/10
6,222,916 B1	*	4/2001	Cameron et al.	379/207.03

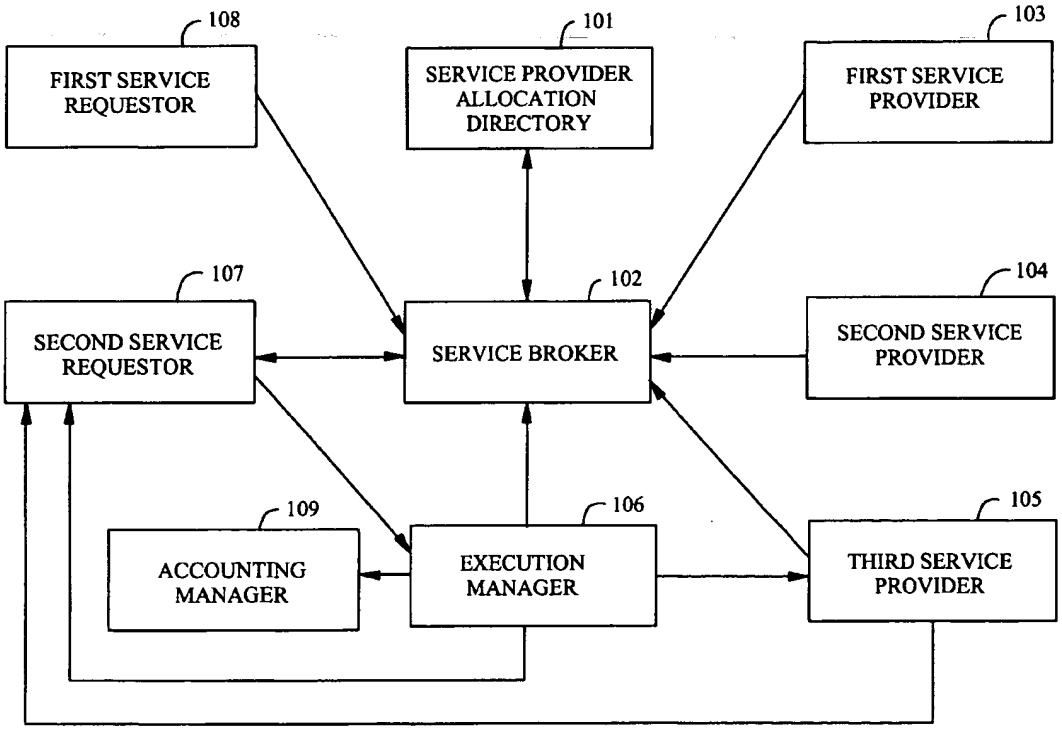
* cited by examiner

Primary Examiner—Greta L. Robinson
(74) *Attorney, Agent, or Firm*—Morgan, Lewis & Bockius, LLP

(57) **ABSTRACT**

A system and a method for managing, organizing, and allocating service providers in the operational environment of a distributed computer network by applying trade and price mechanisms to a plurality of resource allocation decisions. Local resource allocation rules are set forth for maintaining a near-optimal, global load distribution. The service providers are dynamically allocated based upon the supply of the providers and the demand thereof. An automated mechanism, based on service provider reputation, channels demand away from failing or broken service providers. Strategic load balancing rules cause the elimination of ineffective service providers, and also provide a dynamic replication of service providers that cannot handle the current demand. Further, a method for managing the overall system behavior utilizes administrative surcharges.

31 Claims, 6 Drawing Sheets



L8: Entry 2 of 8 File: USPT Oct 1, 2002

DOCUMENT-IDENTIFIER: US 6460082 B1
TITLE: Management of service-oriented resources across heterogeneous media servers using homogenous service units and service signatures to configure the media servers

Brief Summary Text (26):
It is also an object of the present invention to allow the meta-resource to remain autonomous. Thus, according to the principles of the invention, by providing application-level access control onto a meta-resource, the autonomy of meta-resources is preserved. To this end, each service unit is associated with metadata referred to as a "service signature" which is implemented to customize the service commitment of a meta-resource, e.g., by delivering hints to the meta-resource about resource management. For example, the service signature could be used to define access rights and characteristics for any particular service unit. Similarly, the service signature may recommend run-time compensation strategies to be used to update the resource envelope for this service unit under this meta-resource type at different loads. Thus, the service signature is one of the ways in which the present invention allows the integration of service management with resource management.

Detailed Description Text (15):
Similarly, a skilled artisan will appreciate that the meta-resource needs to be trusted by the remote authority and vice-versa. Security when accessing a meta-resource is important to the content subscriber. A mechanism is needed to enforce trust between the different parties. According to today's best practices, a key-exchange mechanism such as RSA may be used to handshake with a resource provider and authenticate the resource provider. Such mechanism is applicable to any other party. Security about the content being accessed is additionally important to the content provider. Thus, enforcement of copyrights and other forms of intellectual property protection over content is necessary. A skilled artisan will appreciate that this is a recognized need and means may be deployed to facilitate the enforcement of copyright between parties having different levels of trustiness. In particular, digital watermarking techniques may be used for safeguarding the copyrights of service objects.

Detailed Description Text (25):
Via access controls over capabilities and service units, the resource provider is now enabled to grant or deny access to the download of capabilities as well as the administration and configuration of its resources into service units.

Detailed Description Text (30):
FIG. 8(a) is a flow chart depicting in greater detail the process for handling a provisioning request (800). As shown in FIG. 8(a), the signaling adapter receives the provisioning request and then forwards any such request to the SUMM which then interfaces to the service unit database in order to retrieve and update resource envelopes (805). At step (810), the service unit signature for the particular requested service is compared with resources at a particular server. Specifically, when a request arrives at the meta-resource, it is necessary to determine whether the request can be serviced, i.e., if the meta-resource is capable, has the resources, is willing to, and has the necessary capability. All these decisions are abstracted by the service unit. Therefore, a determination is made at step (815) as to whether a service unit in a meta-resource is present indicating that the server is capable of provisioning such unit, i.e., that the necessary resources are present. The presence of a service unit provides the ability to determine the willingness of the server in accepting a request. If the service unit is not present, the request fails and the process ends without fulfillment of the request.

If the service unit is present, then at step (820) a determination is made as to whether the meta-resource is willing to accept the request, i.e., if the server is willing to provide the media service when criteria such as price, current service unit utilization, and access controls, for example, are considered. Specifically, after a request arrives to the meta-resource, the meta-resource must decide whether to service the request or not. Such decision is supported by the meta-data in the resource. For example, the meta-resource (i.e., the server) determines whether the requests is associated with the right access controls (permissions) to use the service/storage bins being requested. Other criteria are price/cost admissibility. For example, the request may bound cost to $4.00 for example, whereas the meta-resource is willing to provide the service at $3.00. At step (825) the process will terminate if the request is not admissible, or, will continue otherwise. At step (835) any resource envelope adjustments are made and, at step (840), the adjusted service unit is allocated. For example, a service request may request a service unit (X, Y, Z) resource units of respective resources and is currently being serviced. A second request requests (X, Y, Z). For the adjustment step (835), a heuristics database look-up is performed and a determination made as to the form of the resulting resource allocation (f(X), g(Y), h(Z)) given the class of server (meta-resource). Once the resources are determined, any extra resources can be transferred to the overflow pool (e.g., for the duration associated for the provisioning of this request). This is accomplished during step (840) as well. Then, at step (850) the resource monitors are invoked by the operating system of the provisioning meta-resource (server) to monitor actual resources utilized in the provisioning of the requested service which is provided to the client as indicated at step (855). After provisioning of the service, the process ends at step (860) and returns to process more requests at step (865). Typically, the SUMM (FIG. 7) renders all its comparisons and determinations based on the corresponding resource envelope associated with a particular request and then requests the coordination and allocation of the service unit. However, the coordination between the various resources associated with a particular service unit is provided by the coordinated resource management module (730). In turn, the coordinated resource management module interfaces with the resource management interfaces (750) provided by the operating system found on the meta-resource.

Current US Original Classification (1):
709/226

Current US Cross Reference Classification (1):
709/223

Current US Cross Reference Classification (2):
709/224

Current US Cross Reference Classification (3):
709/225

US006460082B1

(12) **United States Patent**
Lumelsky et al.

(10) **Patent No.: US 6,460,082 B1**
(45) **Date of Patent: Oct. 1, 2002**

(54) **MANAGEMENT OF SERVICE-ORIENTED RESOURCES ACROSS HETEROGENEOUS MEDIA SERVERS USING HOMOGENOUS SERVICE UNITS AND SERVICE SIGNATURES TO CONFIGURE THE MEDIA SERVERS**

(75) Inventors: **Leon L. Lumelsky**, Stamford, CT (US); **Nelson R. Manohar**, New York, NY (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/335,274**

(22) Filed: **Jun. 17, 1999**

(51) **Int. Cl.**[7] **G06F 15/173**
(52) **U.S. Cl.** **709/226**; 709/223; 709/224; 709/225
(58) **Field of Search** 709/223, 224, 709/225, 226, 328

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,442,791	A *	8/1995	Wrabetz et al.	709/330
5,826,239	A *	10/1998	Du et al.	705/8
5,999,525	A *	12/1999	Krishnaswamy et al.	370/352
6,058,423	A *	5/2000	Factor	709/226
6,085,030	A *	7/2000	Whitehead et al.	709/203
6,175,878	B1 *	1/2001	Seaman et al.	709/315
6,216,173	B1 *	4/2001	Jones et al.	709/328

FOREIGN PATENT DOCUMENTS

EP	0 674 280 A2	9/1995
EP	0 834 809 A2	4/1998
EP	0 848 334 A1	6/1998
WO	WO 92/1420	8/1992
WO	WO 93/20511	10/1993
WO	WO 98/15903	4/1998
WO	WO 99/44121	9/1999

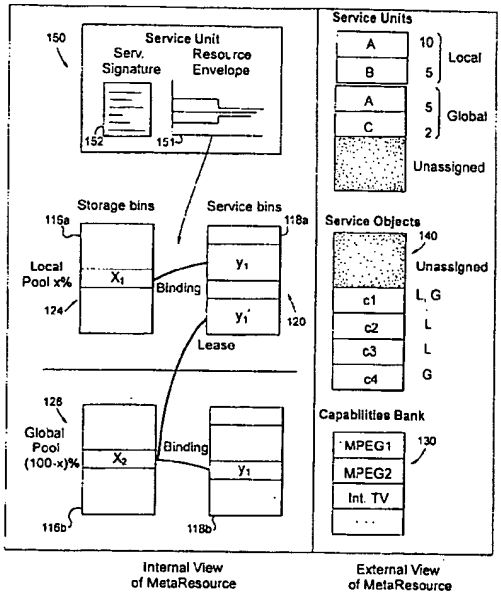
* cited by examiner

Primary Examiner—Zarni Maung
Assistant Examiner—Nabil El-Hady
(74) *Attorney, Agent, or Firm*—Scully, Scott, Murphy & Presser; Douglas W. Cameron

(57) **ABSTRACT**

A system and method for configuring service-oriented resources suitable for the resource management in a media server and more particularly, for resource configuration across distributed media servers. Heterogeneous media serves are configured in terms of homogeneous service-oriented resource units each used to represent a resource allocation commitment from a participating server for provisioning a particular media service on demand. A service unit associated with each different service supported by a media server represents an envelope of resource requirements as needed for provisioning a service. The method includes generating a resource envelope, and additionally compensating, at a media server, for differences between true resource utilization and resource envelope projected by a service unit. Each service unit also comprises a signature representing metadata used to control access to a service unit by defining rights, privileges, and characteristics of services that may use that particular server unit.

24 Claims, 8 Drawing Sheets



L8: Entry 3 of 8 File: USPT Jun 18, 2002

DOCUMENT-IDENTIFIER: US 6408336 B1
TITLE: Distributed administration of access to information

Drawing Description Text (16):
FIG. 15 is a schema of the part of access control database 301 that defines sites in the VPN and the servers, services, and resources at each site;

Detailed Description Text (84):
Thus, in FIG. 4, access filter 403(1) uses its own copy of access control database 301 to determine whether the user who originates a session has access to the information resource specified for the session. If access filter 403(1) so determines, it authenticates the session's outgoing messages and encrypts them as required to achieve the proper trust level. Access filters 403(2..5) then permit the session to proceed because the session is from access filter 403(1) and has been encrypted with SKIP and neither decrypt the messages nor check them using their own copies of access control database 301. Access filter 403(5) then decrypts the messages, confirms that they were encrypted and therefore checked by access filter 403(1), and if the messages are intact, forwards them to server 407 that contains the desired resource. Messages in the session which pass between server 407 and user system 401 are treated in the same way, with access filter 403(5) encrypting them if necessary, access filters 403(2..4) passing them through on the basis of the authentication by 403(5), and access filter 403(1) passing the message on to system 401 on the basis of the authentication and decrypting the message if necessary.

Detailed Description Text (92):
An important task in access control in a VPN is determining the minimum amount of security needed by a session. This is important first because at least that minimum must be guaranteed and second because more security than is necessary wastes resources. The techniques employed in access filters 203 to determine the minimum amount are collectively termed SEND (Secure Encrypted Network Delivery). In SEND, access control database 301 contains a data sensitivity level for each information resource. The data sensitivity level indicates the level of secrecy associated with the information resource and is assigned to the information resource by the security administrator responsible for the resource. An exemplary set of levels is Top Secret, Secret, Private, and Public.

Detailed Description Text (120):
FIG. 7 provides an example of how the sensitivity level of an information resource, the trust level of the user identification, and the trust level associated with the path between the client and the server affect access by the user to the information resource. In FIG. 7, a SKIP-equipped user at client 703 initiates a session 701 to obtain an information resource 723 which is stored at SKIP-equipped server 705. Segment (a) of the above discussion appears in FIG. 7 at 707; segment (b) appears at 709(1..4); Segment (c) appears at 711. Information resource 723 has a sensitivity level of "secret". The first access filter 203 that the session encounters is filter 203(1). Access filter 203(1) uses its copy of the access control database to determine the sensitivity level of resource 723. Here, the user has used a SKIP certificate and an examination of SEND table 601 in data base 301 shows access filter 203(1) that this kind of user identification meets the requirements for information resources having the "secret" sensitivity level, so segment (a) 707 has the required trust level. Consequently, the first access filter goes on to determine the trust level of segments (b) 709(1..4) and (c) between access filter 203(1) and server 705 in the VPN. Segment 709 has subsegments 709(1), 709(2), 709(3), 709(4), and 709(5), and first access filter 203(1) checks the trust level of each of th subsegments in database 301. Segment 709(2) is Internet 121, so its trust level is

"public", which is the minimum in segment 709. Then access filter 203(1) uses access control data base 301 to check the trust level of segment 711. It is "secret". Thus, only segment (b) 709 has a trust level that is too low for the path of a session that is accessing a "secret" information resource 703. To deal with this problem, access filter 103(1) must encrypt the session to bring it up to the necessary trust level. First access filter 203(1) consults SEND table 601 to determine what kind of encryption is required, and row 609(2) indicates that DES encryption is sufficient. First access filter 203(1) accordingly encrypts the session using that algorithm and sends it to access filter 203(5).

Detailed Description Text (151):
When the request is received in access filter 203(c), IP filter 2419 forwards it to Web proxy 2421, which in turn forwards it to Web server 2423, which responds to the request by downloading IntraMap applet 2411 to Web browser 2429 in work station 2403, where IntraMap applet 2411 begins executing in Web browser 2429. During execution, it sends a request to IntraMap proxy 2427 for IntraMap information 2422. Like all Java applets, IntraMap applet 2411 sends the request to the server that it is resident on, in this case, access filter 203(c). However, as with any other request from workstation 2403, the request goes by way of local access filter 203(I). There, IntraMap proxy 2427 detects that the request is addressed to IntraMap proxy 2427 in access filter 203(c) and instead of sending the request on to access filter 203(c), obtains IntraMap information 2422 from the local copy of access control data base 301 in local access filter 203(I), filters it so that it specifies only those resources belonging to the information sets to which the user groups to which the user belongs have access to make to list 2431 and returns it via LAN 213 to IntraMap applet 2411, which then uses list 2431 to make IntraMap display 1801. In making the display, applet 2411 applies any filters specified in the request and also sorts the list as specified in the request. List 2431 not only indicates the resources that are available, but also contains information needed to fetch the resource. Thus, if the resource has a hyperlink, the hyperlink is included in the list; if it is a resource for which the user presently does not have access, but to which the user may request access, the list includes the name and email address of the administrator for the resource.

Detailed Description Text (160):
FIG. 14 shows the schema 1401 for the tables that define information sets. These tables relate information sets (resource groups in FIG. 14) to the resources that make them up and to the network locations of the resources and also organize the information sets into the hierarchical list of information sets displayed at 1003 of FIG. 10. Each information set in access control database 301 is represented by a table of class resource group 1403. Tables of class resource group are organized into a hierarchy for inheritance and display purposes by tables 1419. The relationship between an information set and the resources that make it up on one hand and the locations in the VPN in which they are stored are established by tables of class resource group elements 1407. A table of class resource group may be linked to any number of tables of class resource group elements. A table of class resource group elements is linked to any number of tables of the classes Site Elements 1411, Services 1413, and Resources 1409. There is a table of class Resources for every resource represented in database 301. Included in the table are the resource's ID, its name, the ID for the service that provides it, an ID for a definition of the resource's sensitivity level, a description of the resource, the email address of the administrator of the resource and a hidden flag which indicates whether IntraMap should display the resource to users who do not belong to user groups that have access to the resource. The IntraMap interface obtains the information it needs about a resource from the Resources table for the resource.

Detailed Description Text (318):
Administrators can employ the graphical user interfaces disclosed herein to administer the access control data base. The clarity and ease of use of these graphical user interfaces makes it easy to delegate administrative authority to non-specialists. When an administrator makes a change in the access control data base, the change is first made in the local copy of the data base for a given access filter and then propagated to the local copies of the other access filters. The local copy of the access control database also makes it possible to efficiently implement a graphical user interface to the virtual private network which shows a

user only those resources that belong information sets to which the user groups to which the user belongs have access.

Current US Original Classification (1):
709/229

CLAIMS:

1. An access filter that administers objects including a plurality of information resources and controls access by a user to an information resource of the plurality, the access filter comprising:

access control information including

at least one object that specifies an explicitly-defined set of users,

at least one object that specifies an explicitly-defined set of information resources,

at least one object that specifies an explicitly-defined access policy, the access policy defining access by a defined set of users to a defined set of information resources, and

at least one object that specifies an explicitly-defined administrative policy the administrative policy defining administrative access by a defined set of users to an object; and

an access checker that responds to a request by a user to access a resource or to administer an object by determining from the access control information whether the requesting user may access the requested resource or administer the requested object, the access checker being one of a plurality thereof in a network, having a local copy of the access control information, and employing the local copy to check access.

3. The access filter set forth in claim 1 wherein:

the user employs a client to request access to the information resource;

the client includes a browser which display; a list information resources accessible to the user according to the access policy; and

the access checker uses the access control information to determine which information resources are on the list for the browser.

23. An access control system that controls access by users to information resources, the access control system comprising:

access control information including

at least one object that specifies an explictly-defined set of users as a subset of another set of users and

at least one object that specifies an explicitly-defined set of information resources as a subset of another set of information resources, the sets of users and the sets of information resources being organized hierarchically according to their subset relations; and

at least one object that specifies an explicitly-defined access policy, the access policy defining access by a defined set of users to a defined set of information resources, an access policy for a given user subset and a given information resource subset applying to user sets that are below the given user set in the given user set's hierarchy and to information resource subsets that are below the given information resource set in the given information resource set's hierarchy; and

an access checker which responds to a request by a user for access to the

information resource by determining from the access control information whether the requesting user may access the requested information resource.

36. The access control system set forth in claim 23 wherein the access checker further comprises:

an information resource information provider for a browser employed by the user to view a list of set of information resources accessible to the user, the information resource information provider using the access control information to provide information about which of the sets of information resources are accessible to the user to the browser.

US006408336B1

(12) **United States Patent**
Schneider et al.

(10) **Patent No.: US 6,408,336 B1**
(45) **Date of Patent: *Jun. 18, 2002**

(54) **DISTRIBUTED ADMINISTRATION OF ACCESS TO INFORMATION**

(76) Inventors: **David S. Schneider**, 5338 Hinton Ave., Woodland Hills, CA (US) 91367; **Michael B. Ribet**, 3525 Cass Ct. #617, Oak Brook, IL (US) 60523; **Laurence R. Lipstone**, 22724 Sparrow Dell Dr., Calabasas, CA (US) 91302; **Daniel Jensen**, 6853 Encino Ave., Van Nuys, CA (US) 91406

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/034,507**

(22) Filed: **Mar. 4, 1998**

Related U.S. Application Data

(60) Provisional application No. 60/039,542, filed on Mar. 10, 1997, and provisional application No. 60/040,262, filed on Mar. 10, 1997.

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 9/00

(52) **U.S. Cl.** **709/229**; 713/201

(58) **Field of Search** 709/225, 229; 713/201; 345/335, 969, 741–743

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,956,769	A *	9/1990	Smith	707/1
5,012,405	A *	4/1991	Nishikado et al.	707/8
5,263,157	A *	11/1993	Janis	707/1
5,263,158	A *	11/1993	Janis	711/163
5,263,165	A *	11/1993	Janis	707/1

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

WO	WO 96 05549 A	2/1996	G06F/1/00

OTHER PUBLICATIONS

Computer Dictionary, 2d ed., Microsoft Press, Redmond, Washington, p. 215, Oct. 1993.*

(List continued on next page.)

Primary Examiner—Zarni Maung
Assistant Examiner—Andrew Caldwell
(74) *Attorney, Agent, or Firm*—Gordon E. Nelson

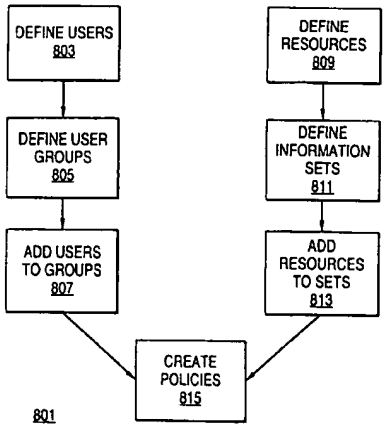
(57) **ABSTRACT**

A scalable access filter that is used together with others like it in a virtual private network to control access by users at clients in the network to information resources provided by servers in the network. Each access filter use a local copy of an access control data base to determine whether an access request made by a user. Changes made by administrators in the local copies are propagated to all of the other local copies. Each user belongs to one or more user groups and each information resource belongs to one or more information sets. Access is permitted or denied according to of access policies which define access in terms of the user groups and information sets. The rights of administrators are similarly determined by administrative policies. Access is further permitted only if the trust levels of a mode of identification of the user and of the path in the network by which the access is made are sufficient for the sensitivity level of the information resource. If necessary, the access filter automatically encrypts the request with an encryption method whose trust level is sufficient. The first access filter in the path performs the access check and encrypts and authenticates the request; the other access filters in the path do not repeat the access check.

48 Claims, 31 Drawing Sheets

U.S. PATENT DOCUMENTS

5,652,787	A *	7/1997	O'Kelly	379/112
5,720,033	A *	2/1998	Deo	713/200
5,787,427	A *	7/1998	Benantar et al.	707/9
5,787,428	A *	7/1998	Hart	707/9



L8: Entry 4 of 8 File: USPT May 28, 2002

DOCUMENT-IDENTIFIER: US 6397336 B2
TITLE: Integrated network security access control system

Abstract Text (1):
A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (2):
The present invention relates in general to data processing and communication systems, and is particularly directed to a data communication security access control mechanism, that is comprised of an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicates with one or more information resources within the network. The security access control mechanism of the invention includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (5):
As a reduced complexity, non-limiting example, FIG. 1 diagrammatically illustrates a network user workstation 10 which is coupled via a communication link 11 to a local area network (LAN) 20 by way of a LAN interface 13. LAN interface 13 also provides access to an external network, such as a public communication services (PCS) network, including the Internet 30, that provides potential access to any network information resource (e.g., processor-accessible digital database). The local area network 20 to which user 10 is connected customarily includes one or more computer-based units, such as the illustrated workstations 21 and 22, network server 23 and printer 24, which are interconnected via a hub 25. The hub 25 is connected to the LAN interface 13, so that the end user workstation 10 may access any `local` information resource of the LAN 20. In order to connect to the external network 30, the network interface 13 may be coupled through an electronic mail gateway 32 and a modem 33, whereby a dial-up connection may be provided to an Internet connection or other global resource provider 34, through which access to any node in the overall network is achieved.

Brief Summary Text (6):
Because the network provides a potential window into any information resource linked to any of its nodes, it is customary to both wrap or embed all communications in a `security blanket` (some form of encryption) at a communication sourcing end, and to employ one or more permission (authorization and authentication) layers that must be used to gain access to another system resource (e.g., another computer). Once installed, such schemes operate as micro security systems, primarily as binary

permission filters--the user is either permitted or denied access to a destination information resource, and are customarily limited to a relatively limited (and often fixed) set of access permission criteria. Now, while such schemes provide some measure of access control, they do not provide a macro perspective or control of all of the resources for which a given network security system may be configured.

Brief Summary Text (8):
In accordance with the present invention, this problem is effectively remedied by a new and improved network resource security access control mechanism that includes protection control, access control, event management and a pro-active security agent routines integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Detailed Description Text (2):
Before describing in detail the new and improved network resource security access control mechanism in accordance with the present invention, it should be observed that the present invention resides primarily in what is effectively a new and improved data security access control mechanism implemented as an arrangement of abstract security services. These abstract security services include protection control, access control, event management and a pro-active security agent that are integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network. The particular resources and the information they provide, per se, are not considered part of the invention.

Detailed Description Text (4):
Attention is now directed to FIG. 2, which shows a reduced complexity, non-limiting example of an information resource network 100 having a plurality of resource nodes 110, to which one or more information resource objects, such as respective computers 120 used by user's to couple to and process data transported over the network, may be coupled, and communications among which are supervised or controlled by a network resource security services control system 200. As pointed out briefly above, and as will be detailed infra, network resource security services control system 200 communicates with each of resource and communication control objects, and includes a protection control routine 220, and access control routine 230, and event manager 240 and a pro-active security agent routine 250, which interact with one another and with network resources, so as to control the ability of network users to gain access to, transmit and retrieve information with respect to any of the resources of the network.

Detailed Description Text (9):
An object is any potential participant in the system, such as a user, information resource, communication path, protection mechanism (such as a cryptography algorithm or user's authentication procedure within the protection control routine 220), an access control feature of the access control routine 230, etc.

Detailed Description Text (18):
As will be appreciated from the foregoing description, the network resource security services control system of the present invention provides an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. This security access control mechanism includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Current US Cross Reference Classification (1):
709/229

CLAIMS:

3. The method according to claim 1, wherein step (c) comprises monitoring information generated by events associated with said user's being selectively granted access to said resource in step (b), and wherein step (d) comprises, in response to information generated by said events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, diminishing the ability of said user to access a network resource.

4. The method according to claim 1, wherein said security relationships among said users and resources of said information network include a protection control routine containing a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among said users and resources of said network, and wherein step (d) comprises modifying one or more of said security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to increase the difficulty of said user to access a network resource.

8. The mechanism according to claim 6, wherein step (b) comprises monitoring information generated by events associated with said user being selectively granted access to said resource in step (a) and, wherein step (c) comprises, in response to information generated by said events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, diminishing the ability of said user to access a network resource.

9. The mechanism according to claim 6, wherein said security relationships among said users and resources of said information network include a protection control routine containing a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among said users and resources of said network, and wherein step (c) comprises modifying one or more of said security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to increase the difficulty of said user to access a network resource.

US006397336B2

(12) **United States Patent**
Leppek

(10) **Patent No.: US 6,397,336 B2**
(45) **Date of Patent: *May 28, 2002**

(54) **INTEGRATED NETWORK SECURITY ACCESS CONTROL SYSTEM**

(75) Inventor: **James Leppek**, Melbourne, FL (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/740,295**

(22) Filed: **Dec. 19, 2000**

Related U.S. Application Data

(63) Continuation of application No. 09/391,306, filed on Sep. 7, 1999, now Pat. No. 6,189,104, which is a continuation of application No. 09/054,705, filed on Apr. 3, 1998, now Pat. No. 5,974,149, which is a continuation of application No. 08/690,784, filed on Aug. 1, 1996, now Pat. No. 5,787,177.

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/201**; 713/154; 709/229
(58) **Field of Search** 713/201, 153, 713/154; 707/9; 709/229

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,245,045	A	4/1966	Randlev	395/866
3,798,605	A	3/1974	Feistel	380/25
3,858,182	A	12/1974	Delagi et al.	395/186
3,931,504	A	1/1976	Jacoby	395/186
4,827,508	A	5/1989	Shear	380/4
4,961,224	A	10/1990	Yung	380/25
5,204,961	A	4/1993	Barlow	395/725
5,787,177	A	7/1998	Leppek	380/25
5,974,149	A *	10/1999	Leppek	380/25
6,088,451	A *	7/2000	He et al.	380/25
6,125,390	A *	9/2000	Touboul	709/223
6,189,104	B1 *	2/2001	Leppek	713/201

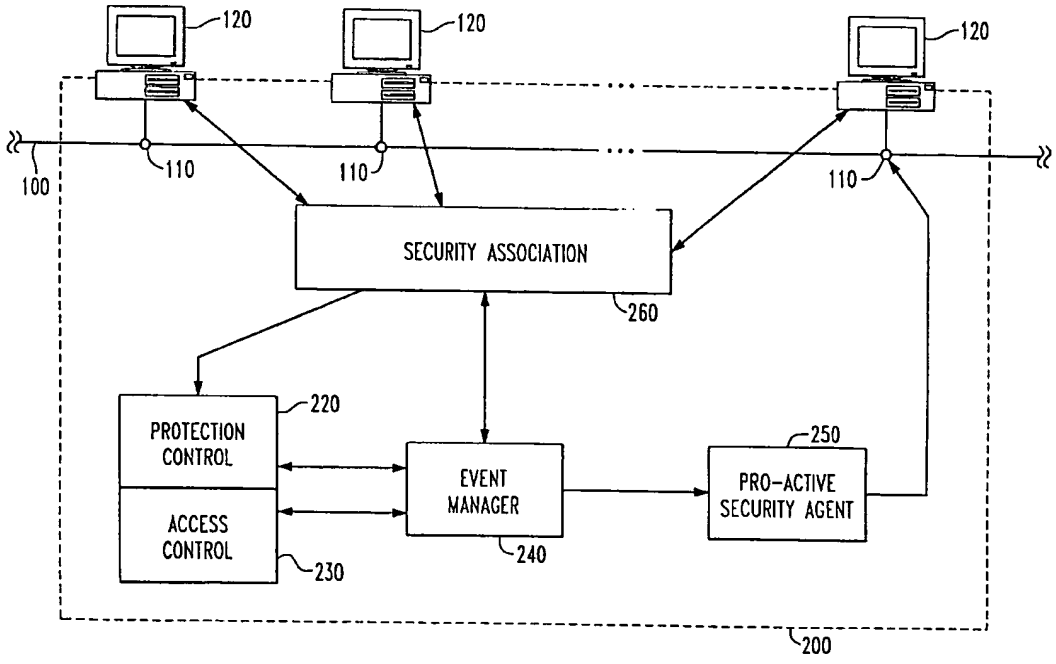
* cited by examiner

Primary Examiner—Robert Beausoleil
Assistant Examiner—Scott T. Baderman
(74) *Attorney, Agent, or Firm*—Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

10 Claims, 2 Drawing Sheets



L8: Entry 5 of 8 File: USPT May 22, 2001

DOCUMENT-IDENTIFIER: US 6237023 B1
**** See image for Certificate of Correction ****
TITLE: System for controlling the authority of a terminal capable of simultaneously operating a plurality of client softwares which transmit service requests

Brief Summary Text (2):
This invention relates to an access control system and method, particular access control of a distributed system in which the resources of remote sites are shared using a computer network, by way of example.

Brief Summary Text (3):
Access control in a distributed system generally is achieved by combining an authentication mechanism in the distributed system with a resource protection mechanism at each site. For example, a distributed file system, which is a means of sharing files via a network, is used in a comparatively small-scale network environment such as a local area network (LAN). In such case user authentication means at the site level is appropriated in the network environment as well by unifying modes of user management, and resource protection is achieved based upon the authority granted to authenticated users. The file access control means for implementing this generally is provided by the operating system (OS).

Brief Summary Text (6):
The first problem is that satisfactory reliability cannot be assured merely by applying the site-level user authentication mechanism to a distributed system. Even if modes of user management are unified between sites, no legal force is involved and a certain site is capable of individually altering some of the management information. In cases such as these, it is possible for a site administrator to impersonate a user and it is difficult for the resource provider to detect this.

Brief Summary Text (9):
Accordingly, an object of the present invention is to provide an access control system and method in which, when shared resources in a distributed system are accessed, the shared resources can be protected safely and flexibly.

Brief Summary Text (10):
According to the present invention, the foregoing object is attained by providing an access control system for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising acquisition means for acquiring an identifier of a terminal-which requests a service and an identifier of a user, decision means for uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and judging means for judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (11):
In another aspect of the invention, the foregoing object is attained by providing an access control system for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising relay means for acquiring an identifier of a user requesting a service, intercepting the service request by transmitting, to a prescribed address, a service request message onto which the acquired user identifier has been added, and distributing a received message, and service providing means for acquiring as a user identifier an identifier added onto the received service request message, acquiring as a terminal identifier an identifier of the relay means that transmitted this service request message, uniquely deciding authority over the service request based upon the

terminal identifier and user identifier that have been acquired, and judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (12):
According to the present invention, the foregoing object is attained by providing an access control method for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising an acquisition step of acquiring an identifier of a terminal which requests a service and an identifier of a user, a decision step of uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and a judging step of judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (13):
In another aspect of the invention, the foregoing object is attained by providing an access control method for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising, in relay means for intercepting a service request and distributing a received message, a first acquisition step of acquiring an identifier of a user requesting a service and a transmission step of transmitting, to service providing means, a service request message to which the acquired user identifier has been added on, and, in the service providing means, a receiving step of receiving a service request message, a second acquisition step of acquiring as a user identifier the identifier added onto the received service request message, and acquiring is a terminal identifier an identifier of the relay means that transmitted this service request message, a decision step of uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and a judging step of judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (14):
In accordance with the present invention having the configuration described above, it is possible to provide an access control system and method in which, when shared resources in a distributed system are accessed, the shared resources can be protected safely and flexibly.

Current US Original Classification (1):
709/203

Current US Cross Reference Classification (1):
709/201

US006237023B1

(12) **United States Patent**
Yoshimoto

(10) **Patent No.: US 6,237,023 B1**
(45) **Date of Patent: May 22, 2001**

(54) **SYSTEM FOR CONTROLLING THE AUTHORITY OF A TERMINAL CAPABLE OF SIMULTANEOUSLY OPERATING A PLURALITY OF CLIENT SOFTWARES WHICH TRANSMIT SERVICE REQUESTS**

(75) Inventor: **Masahiko Yoshimoto**, Yokohama (JP)

(73) Assignee: **Canon Kabushiki Kaisha**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **08/873,104**

(22) Filed: **Jun. 11, 1997**

(30) **Foreign Application Priority Data**

Jun. 14, 1996 (JP) 8-154118

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/203**; 709/201; 713/200; 713/201; 713/202

(58) **Field of Search** 395/186, 187.01, 395/200.25, 188.01, 210.3, 200.57; 370/427, 446; 380/23, 25; 713/200, 201, 202; 709/203, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,672,572		6/1987	Alsberg	364/900
4,891,838		1/1990	Faber	380/25
4,896,319	*	1/1990	Lidinsky et al.	370/427
4,916,738		4/1990	Chandra et al.	380/25
5,261,070		11/1993	Ohta	395/425
5,278,904	*	1/1994	Servi	380/23
5,590,199	*	12/1996	Krajewski et al.	380/25
5,706,427	*	1/1998	Tabuki	395/200.57
5,815,664	*	9/1998	Asano	395/200.57
5,841,970	*	11/1998	Tabuki	713/201

FOREIGN PATENT DOCUMENTS

0604911 A2 12/1993 (EP) .

OTHER PUBLICATIONS

Tanenbaum, A.S. et al. "The Amoeba distributed operating system—a status report", Computer Communications 14 (1991) Jul./Aug., No. 6, London,GB.

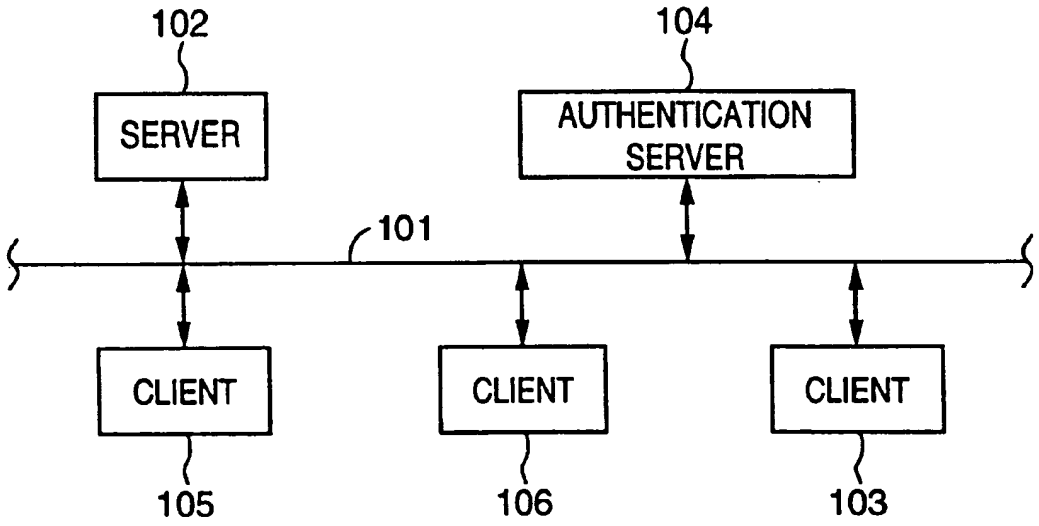
* cited by examiner

Primary Examiner—Meng-Al T. An
Assistant Examiner—Nabil El-Hady
(74) *Attorney, Agent, or Firm*—Fitzpatrick, Cella, Harper & Scinto

(57) **ABSTRACT**

When a server receives a service request from a client, identifiers of a terminal and of a user are acquired from the service request and authority with respect to the service request is uniquely decided from the terminal and user identifiers acquired. It is then determined, using the authority decided, whether or not to accept the service request.

84 Claims, 6 Drawing Sheets



DOCUMENT-IDENTIFIER: US 6189104 B1
TITLE: Integrated network security access control system

Abstract Text (1):
A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (2):
The present invention relates in general to data processing and communication systems, and is particularly directed to a data communication security access control mechanism, that is comprised of an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism of the invention includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (5):
As a reduced complexity, non-limiting example, FIG. 1 diagrammatically illustrates a network user workstation 10 which is coupled via a communication link 11 to a local area network (LAN) 20 by way of a LAN interface 13. LAN interface 13 also provides access to an external network, such as a public communication services (PCS) network, including the Internet 30, that provides potential access to any network information resource (e.g., processor-accessible digital database). The local area network 20 to which user 10 is connected customarily includes one or more computer-based units, such as the illustrated workstations 21 and 22, network server 23 and printer 24, which are interconnected via a hub 25. The hub 25 is connected to the LAN interface 13, so that the end user workstation 10 may access any `local` information resource of the LAN 20. In order to connect to the external network 30, the network interface 13 may be coupled through an electronic mail gateway 32 and a modem 33, whereby a dial-up connection may be provided to an Internet connection or other global resource provider 34, through which access to any node in the overall network is achieved.

Brief Summary Text (6):
Because the network provides a potential window into any information resource linked to any of its nodes, it is customary to both wrap or embed all communications in a `security blanket` (some form of encryption) at a communication sourcing end, and to employ one or more permission (authorization and authentication) layers that must be used to gain access to another system resource (e.g., another computer). Once installed, such schemes operate as micro security systems, primarily as binary

permission filters--the user is either permitted or denied access to a destination information resource, and are customarily limited to a relatively limited (and often fixed) set of access permission criteria. Now, while such schemes provide some measure of access control, they do not provide a macro perspective or control of all of the resources for which a given network security system may be configured.

Brief Summary Text (8):
In accordance with the present invention, this problem is effectively remedied by a new and improved network resource security access control mechanism that includes protection control, access control, event management and a pro-active security agent routines integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Detailed Description Text (2):
Before describing in detail the new and improved network resource security access control mechanism in accordance with the present invention, it should be observed that the present invention resides primarily in what is effectively a new and improved data security access control mechanism implemented as an arrangement of abstract security services. These abstract security services include protection control, access control, event management and a pro-active security agent that are integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network. The particular resources and the information they provide, per se, are not considered part of the invention.

Detailed Description Text (4):
Attention is now directed to FIG. 2, which shows a reduced complexity, non-limiting example of an information resource network 100 having a plurality of resource nodes 110, to which one or more information resource objects, such as respective computers 120 used by user's to couple to and process data transported over the network, may be coupled, and communications among which are supervised or controlled by a network resource security services control system 200. As pointed out briefly above, and as will be detailed infra, network resource security services control system 200 communicates with each of resource and communication control objects, and includes a protection control routine 220, and access control routine 230, and event manager 240 and a pro-active security agent routine 250, which interact with one another and with network resources, so as to control the ability of network users to gain access to, transmit and retrieve information with respect to any of the resources of the network.

Detailed Description Text (8):
The event manager 240 is a routine that monitors network activity, in particular `events` occurring as a result of activity among users and resources of the network. An event is an activity that occurs when a user executes activity in the network, or as a result of exercising or using a resource or object within the system. An object is any potential participant in the system, such as a user, information resource, communication path, protection mechanism (such as a cryptography algorithm or user's authentication procedure within the protection control routine 220), an access control feature of the access control routine 230, etc.

Detailed Description Text (17):
As will be appreciated from the foregoing description, the network resource security services control system of the present invention provides an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. This security access control mechanism includes monitoring activity associated with user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications

with respect to a system resource.

Current US Cross Reference Classification (1):
709/229

CLAIMS:

5. A method according to claim 1, wherein step (c) comprises monitoring information generated by a plurality of events associated with said network user's accessing said network resource in step (b), and wherein step (d) comprises, in response to information generated by said plurality of events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, decreasing the ability of said network user to access a network resource.

6. A method of controlling the ability of a user to access one or more information resources of an information network comprising the steps of:

(a) providing a protection control routine having a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among users and resources of said network;

(b) selectively permitting a user to access a network resource in accordance with at least one of a plurality of security relationships among users and resources of said information network; and

(c) controllably modifying one or more of said plurality of security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to affect the ability of said user to access a network resource.

US006189104B1

(12) **United States Patent**
Leppek

(10) **Patent No.: US 6,189,104 B1**
(45) **Date of Patent: *Feb. 13, 2001**

(54) **INTEGRATED NETWORK SECURITY ACCESS CONTROL SYSTEM**

(75) Inventor: **James Leppek**, Melbourne, FL (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/391,306**

(22) Filed: **Sep. 7, 1999**

Related U.S. Application Data

(63) Continuation of application No. 09/054,705, filed on Apr. 3, 1998, now Pat. No. 5,974,149, which is a continuation of application No. 08/690,784, filed on Aug. 1, 1996, now Pat. No. 5,787,177.

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/201**; 713/154; 709/229
(58) **Field of Search** 713/201, 153, 713/154; 709/229; 707/9

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,827,508 * 5/1989 Shear 380/4
4,961,224 * 10/1990 Yung 380/25
5,204,961 * 4/1993 Barlow 395/725
5,787,177 * 7/1998 Leppek 380/25

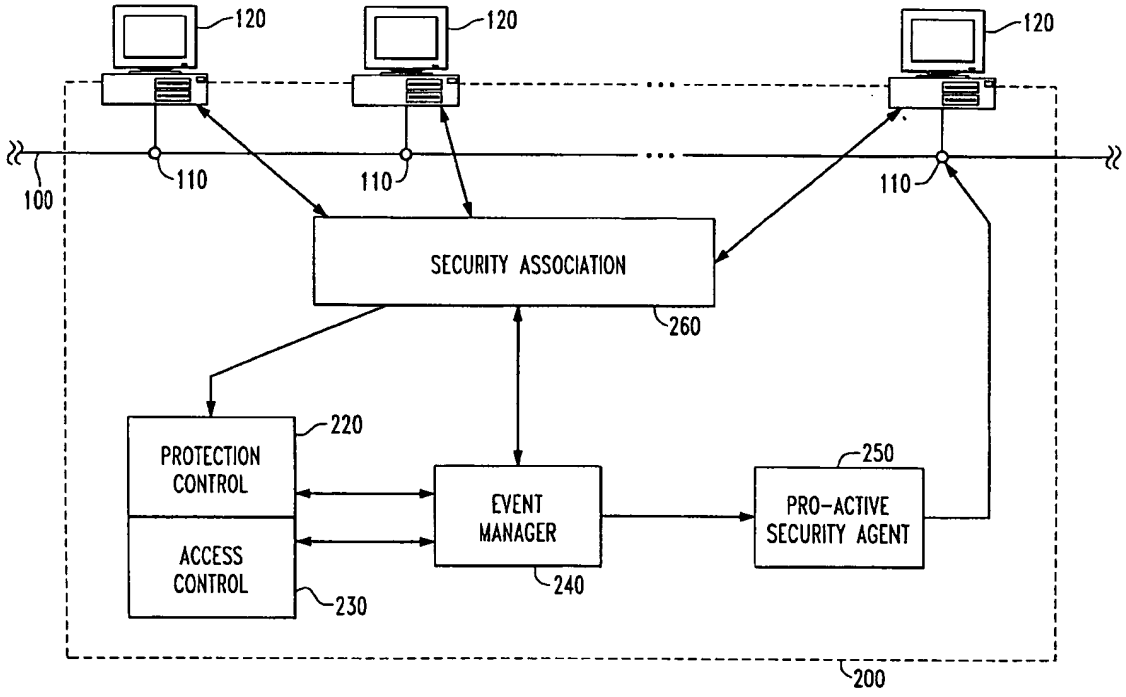
* cited by examiner

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Scott T. Baderman
(74) *Attorney, Agent, or Firm*—Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

8 Claims, 2 Drawing Sheets



DOCUMENT-IDENTIFIER: US 5845255 A
TITLE: Prescription management system

Detailed Description Text (236):
Current and historical reports can, subject to the access controls described herein, be patient-specific, prescriber-specific or organization-specific and can be aggregated across various groups, pools, geographical regions, conditions, drugs, or time periods or combinations of any of the foregoing to provide a valuable data resource to health care providers, patients, managed care organizations, government agencies and others.

Current US Original Classification (1):
705/3

US005845255A

United States Patent [19]

Mayaud

[11] Patent Number: 5,845,255

[45] Date of Patent: Dec. 1, 1998

[54] PRESCRIPTION MANAGEMENT SYSTEM

[75] Inventor: **Christian Mayaud**, New Canaan, Conn.

[73] Assignee: **Advanced Health Med-E-Systems Corporation**, Tarrytown, N.Y.

[21] Appl. No.: **942,372**

[22] Filed: **Oct. 2, 1997**

Related U.S. Application Data

[63] Continuation of Ser. No. 330,745, Oct. 28, 1994, abandoned.

[51] **Int. Cl.**[6] **G06F 159/00**

[52] **U.S. Cl.** **705/3**

[58] **Field of Search** 705/3, 2

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,674,652	6/1987	Aten et al.	221/3
4,695,954	9/1987	Rose et al.	364/413.01
4,766,542	8/1988	Pilarczyk .	
4,847,764	7/1989	Halvorson	364/413.02
4,860,899	8/1989	McKee	206/534
4,991,877	2/1991	Lieberman	283/36
5,065,315	11/1991	Garcia .	
5,072,383	12/1991	Brimm et al. .	
5,084,828	1/1992	Kaufman et al. .	
5,208,762	5/1993	Charhut et al.	364/478
5,292,029	3/1994	Pearson	221/2
5,299,121	3/1994	Brill .	
5,347,453	9/1994	Maestre	364/413.01
5,347,477	9/1994	Lee .	
5,390,238	2/1995	Kirk et al.	379/93
5,502,944	4/1996	Kraft et al.	53/55
5,528,021	6/1996	Lassus et al.	235/380

FOREIGN PATENT DOCUMENTS

40 23 785	1/1992	Germany .

OTHER PUBLICATIONS

Supplementary Partial European Search Report, EP 95 93 7691, Mar. 9, 1998.

"S-O-A-P Drug Interaction Program"; Dialog File 256, Acc. No. 01304468; released Nov. 1987. item (304468) in Directory (Abstract Only).

"EZ-Rx System"; Dialog File 256, Acc. No. 01017836, by Signature Software Systems, Inc., released Apr. 1982 item (017836) (Abstract Only).

"EZ-Rx System"; Dialog File 751 Acc. No. 00268373, by Signature Software Systems, Inc., released Feb. 1982, [DATAPRO] (Abstract Only).

"Newton Software Titles" Brochure, Part No. L00587B, (1994, Apple Computer, Inc.).

"Newton Getting through the day is a business in itself" Brochure, Part No. L00683A, (1994, Apple Computer, Inc.).

"Newton-based units to proliferate in fall", p. 8, PC Week, Aug. 15, 1994 (Ziff-Davies, New York).

"The future of medicine" pp. 1, 4-9, 12-18; The Economist, Mar. 19, 1994.

Abstracts (A-N) and papers (AA-SS) in *1994 Spring Congress Final Program and Abstract Book* (American Medical Informatics Association, Bethsda, MD, Spring Congress May 4-7, 1994, San Francisco); as follows.

(List continued on next page.)

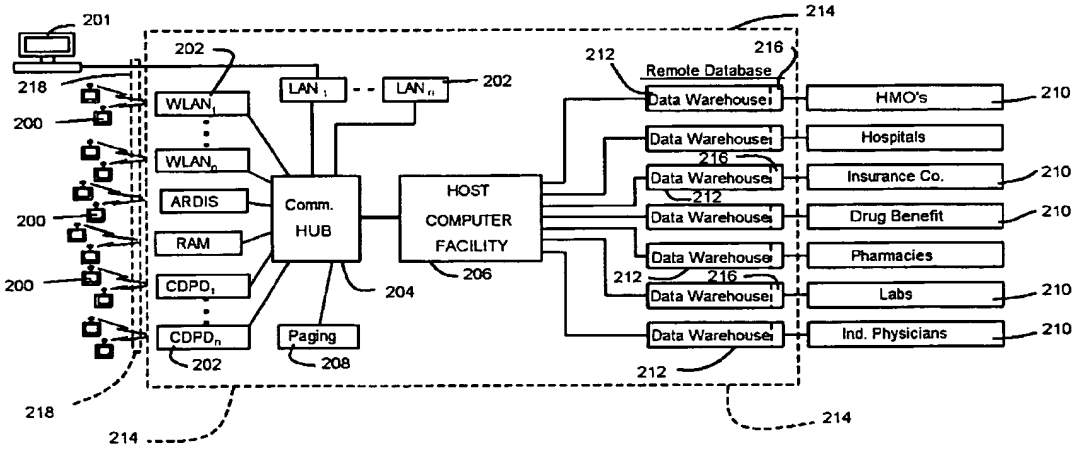
Primary Examiner—Donald E. McElheny, Jr.

Attorney, Agent, or Firm—Handal & Morofsky

[57] ABSTRACT

A wirelessly deployable, electronic prescription creation system for physician use captures into a prescription a patient condition-objective of the prescribed treatment and provides for patient record assembly from source elements, with privacy controls for patient and doctor, adverse indication review and online access to comprehensive drug information including scientific literature. Extensions to novel multi-drug packages and dispensing devices, and an "intelligent network" remote data retrieval architecture as well as onscreen physician-to-pharmacy and physician-to-physician e-mail are also provided.

34 Claims, 21 Drawing Sheets



L8: Entry 8 of 8 File: USPT Apr 7, 1998

DOCUMENT-IDENTIFIER: US 5737539 A
TITLE: Prescription creation system

Detailed Description Text (228):
Current and historical reports can, subject to the access controls described herein, be patient-specific, prescriber-specific or organization-specific and can be aggregated across various groups, pools, geographical regions, conditions, drugs, or time periods or combinations of any of the foregoing to provide a valuable data resource to health care providers, patients, managed care organizations, government agencies and others.

Current US Original Classification (1):
705/3

Current US Cross Reference Classification (1):
705/2

US005737539A

United States Patent [19]

Edelson et al.

[11] Patent Number: 5,737,539

[45] Date of Patent: Apr. 7, 1998

[54] **PRESCRIPTION CREATION SYSTEM**

[75] Inventors: **Jonathan Edelson**, Scarsdale, N.Y.; **Christian Mayaud**, New Canaan, Conn.

[73] Assignee: **Advanced Health Med-E-Systems Corp.**, Tarrytown, N.Y.

[21] Appl. No.: **330,939**

[22] Filed: **Oct. 28, 1994**

[51] **Int. Cl.**[6] **G06F 159/00**; G06F 17/60

[52] **U.S. Cl.** **395/203**; 395/202

[58] **Field of Search** ..... 364/401 M, 401 R, 364/406, 408; 395/203, 202, 228, 229

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,674,652	6/1987	Aten et al.	221/3
4,695,954	9/1987	Rose et al.	364/413.01
4,766,542	8/1988	Pilarczyk .	
4,847,764	7/1989	Halvorson	364/413.02
4,860,899	8/1989	McKee	206/534
4,991,877	2/1991	Lieberman	283/36
5,065,315	11/1991	Garcia .	
5,072,383	12/1991	Brimm et al. .	
5,084,828	1/1992	Kaufman et al. .	
5,208,762	5/1993	Charhut et al.	364/478
5,292,029	3/1994	Pearson	221/2
5,347,453	9/1994	Maestre	364/413.01
5,347,477	9/1994	Lee .	
5,390,238	2/1995	Kirk et al.	379/93
5,502,944	4/1996	Kraft et al.	53/55
5,528,021	6/1996	Lassus et al.	235/380

OTHER PUBLICATIONS

Anonymous, "Data Hard to Get, Has Many Applications," *Employee Benefits Plan Review*, vol. 45, No. 5, pp. 62–65, Nov. 1992.

"Newton Software Titles" Brochure, Part No. L00587B, (1994, Apple Computer, Inc.).

"Newton Getting through the day is a business in itself" Brochure, Part No. L00683A, (1994, Apple Computer, Inc.).

"Newton–based units to proliferate in fall", p. 8, PC Week, Aug. 15, 1994 (Ziff–Davies, New York).

"The future of medicine" pp. 1, 4–9, 12–18; The Economist, Mar. 19, 1994.

Abstracts (A–N) and papers (AA–SS) in 1994 *Spring Congress Final Program and Abstract Book* (American Medical Informatics Association, Bethsda, MD, Spring Congress May 4–7, 1994, San Francisco); as follows:.

"Mobile Computing in the 1990's" by Larry G. Tesler, p. 29.

"Wireless Clinical Computing: Uses and Spinoffs" by Larry Frisch, M.D.

"Health Data: Disclosure, Protection, and Privacy" by Molla S. Donaldson, M.S. et al., p. 39.

"Electronic Signatures: A Dissuasion Strategy to Protect Medical Records Based on Medical Liabilility" by F.A. Allaert and L. Dusserre, p. 40.

"The Trade Off Between Accessibility of Information, The Truthfulness of Medical Records, Etc." by Dr. Ian Purves, et al., p. 41.

(List continued on next page.)

Primary Examiner—Gail O. Hayes
Assistant Examiner—Joseph Thomas
Attorney, Agent, or Firm—Handal & Morofsky

[57] **ABSTRACT**

An electronic prescription creation system for use by professional prescribers at the point of care has a prescription division subsystem permitting creation of a single prescription to be automatically divided into two components for fulfilment of one portion quickly and locally at higher cost and of another portion by remote mail order taking more time but providing a cost saving for a major part of the prescription. The prescription creation system has an ability to access remote source databases for system presentation to the prescriber of relevant, authorized and current drug, drug formulary and patient history information, with dynamic creation of a transient virtual patient record, the information being presented to the prescriber before completion of the prescription, permitting enhancement of the quality of prescribing decisions.

5 Claims, 16 Drawing Sheets